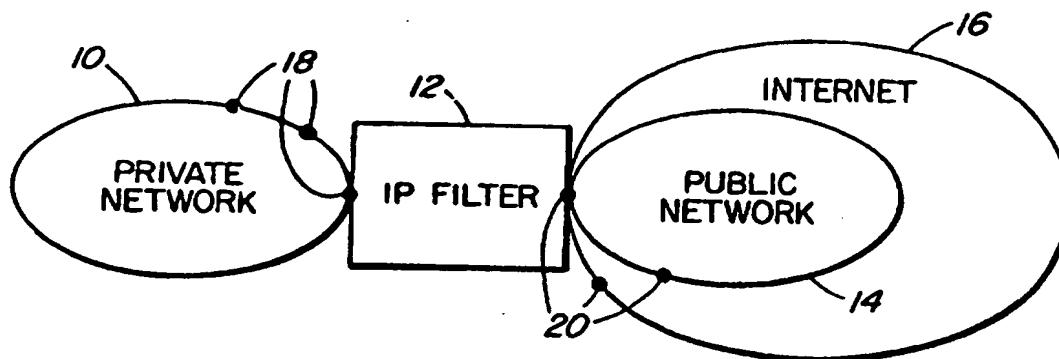




## INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

|  |  |   |   |
|--|--|---|---|
| (51) International Patent Classification <sup>6</sup> :<br><br>H04L 29/06  |  | A2  | (11) International Publication Number: <b>WO 97/40610</b>       |
|  |  |   | (43) International Publication Date: 30 October 1997 (30.10.97) |
| (21) International Application Number: PCT/CA97/00269  |  | (81) Designated States: AU, CA, CN, JP, KR, European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE). |   |
| (22) International Filing Date: 23 April 1997 (23.04.97)   |  |   |   |
| (30) Priority Data:<br>60/015,945 24 April 1996 (24.04.96) US  |  | Published<br><i>Without international search report and to be republished upon receipt of that report.</i>                        |   |
| (71) Applicant: NORTHERN TELECOM LIMITED [CA/CA];<br>World Trade Center of Montreal, 8th floor, 380 St. Antoine<br>Street West, Montreal, Quebec H2Y 3Y4 (CA).     |  |   |   |
| (72) Inventors: WOOTTON, Bruce, Anthony; 10601 Bent Twig<br>Drive, Raleigh, NC 27613 (US). COLVIN, William, G.;<br>874 Childs Drive, Milton, Ontario L9T 4J6 (CA). |  |   |   |
| (74) Agent: GRANCHELLI, John, A.; Northern Telecom Limited,<br>Patent Dept., P.O. Box 3511, Station "C", Ottawa, Ontario<br>K1Y 4H7 (CA).                          |  |   |   |

(54) Title: INTERNET PROTOCOL FILTER



## (57) Abstract

The IP filter (12), embodying the present invention, is a communications device designed to provide public network (14) or Internet (16) access to nodes (18) of private networks (10), advantageously without requiring the private nodes on such networks to register public Internet addresses. The IP filter presents a single IP address to the Internet and uses a plurality of IP ports to solve the problem of IP address conservation. It initiates sessions by assigning private side IP sessions to a unique port of the IP filter's public address. The IP filter effects a translation between a source port number for the private network and a destination port number for the public network for communication therebetween. Benefits of the IP filter include private node security and conservation of Internet-registered addresses.

**FOR THE PURPOSES OF INFORMATION ONLY**

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

|    |                          |    |                                       |    |   |    |                          |
|----|--------------------------|----|---------------------------------------|----|---|----|--------------------------|
| AL | Albania                  | ES | Spain                                 | LS | Lesotho                                   | SI | Slovenia                 |
| AM | Armenia                  | FI | Finland                               | LT | Lithuania                                 | SK | Slovakia                 |
| AT | Austria                  | FR | France                                | LU | Luxembourg                                | SN | Senegal                  |
| AU | Australia                | GA | Gabon                                 | LV | Latvia                                    | SZ | Swaziland                |
| AZ | Azerbaijan               | GB | United Kingdom                        | MC | Monaco                                    | TD | Chad                     |
| BA | Bosnia and Herzegovina   | GE | Georgia                               | MD | Republic of Moldova                       | TG | Togo                     |
| BB | Barbados                 | GH | Ghana                                 | MG | Madagascar                                | TJ | Tajikistan               |
| BE | Belgium                  | GN | Guinea                                | MK | The former Yugoslav Republic of Macedonia | TM | Turkmenistan             |
| BF | Burkina Faso             | GR | Greece                                | ML | Mali                                      | TR | Turkey                   |
| BG | Bulgaria                 | HU | Hungary                               | MN | Mongolia                                  | TT | Trinidad and Tobago      |
| BJ | Benin                    | IE | Ireland                               | MR | Mauritania                                | UA | Ukraine                  |
| BR | Brazil                   | IL | Israel                                | MW | Malawi                                    | UG | Uganda                   |
| BY | Belarus                  | IS | Iceland                               | MX | Mexico                                    | US | United States of America |
| CA | Canada                   | IT | Italy                                 | NE | Niger                                     | UZ | Uzbekistan               |
| CF | Central African Republic | JP | Japan                                 | NL | Netherlands                               | VN | Viet Nam                 |
| CG | Congo                    | KR | Kenya                                 | NO | Norway                                    | YU | Yugoslavia               |
| CH | Switzerland              | KG | Kyrgyzstan                            | NZ | New Zealand                               | ZW | Zimbabwe                 |
| CI | Côte d'Ivoire            | KP | Democratic People's Republic of Korea | PL | Poland                                    |    |                          |
| CM | Cameroon                 | KR | Republic of Korea                     | PT | Portugal                                  |    |                          |
| CN | China                    | KZ | Kazakhstan                            | RO | Romania                                   |    |                          |
| CU | Cuba                     | LC | Saint Lucia                           | RU | Russian Federation                        |    |                          |
| CZ | Czech Republic           | LI | Liechtenstein                         | SD | Sudan                                     |    |                          |
| DE | Germany                  | LK | Sri Lanka                             | SE | Sweden                                    |    |                          |
| DK | Denmark                  | LR | Liberia                               | SG | Singapore                                 |    |                          |

INTERNET PROTOCOL FILTER  
Background Of The Invention

The present invention generally relates to inter-network firewalls and, in particular, to an internet protocol (IP) filter whereby a private IP network domain is mapped to a single IP address on the public Internet.

5 Firewalls are generally known and characterized by computer servers which function to couple nodes within the domain of the private network to nodes in a public network 10 domain, such as the Internet. A deficiency of the known firewall products is the need for a unique public IP address for each concurrent session or interaction between public and private nodes.

15 A firewall providing conservation of public IP addresses would be desirable.

Summary Of The Invention

It is an object of the present invention to provide a new and improved apparatus for communicatively coupling two networks.

20 The invention, therefore, according to a first exemplary aspect provides a method of interfacing private and public data communications networks, through a filter node in communication with both networks, the filter node having an address known in the public network, comprising 25 the steps of: routing from nodes in the private network, to the filter node, data packets having destination information, which includes a destination address and a destination port, corresponding to nodes in the public network and having source information, which includes a 30 source address and a source port, of the respective private network nodes; for each data packet received from the private network, at the filter node, maintaining the source information taken from the data packet in correlation with a unique value representing a port of the filter node, and 35 replacing in the data packet the source address with the filter node address and the source port with the filter node port value; and routing from the filter node, in the

- 2 -

public network, the data packets having the replaced source information, according to the destination information in each, to the corresponding public network nodes.

According to a second exemplary aspect, the

5 invention provides a method of interfacing private and public data communications networks, through a filter node in communication with both networks, comprising the steps of: (a) receiving at the filter node, from the private network, a data packet having an a destination address

10 corresponding to a node in the public network and a source address corresponding to a node in the private network; (b) maintaining, by the filter node, the source address taken from the data packet; (c) replacing, in the data packet, the source address with an address of the filter node; (d)

15 routing from the filter node, in the public network, the data packet having the replaced source address, according to the destination address, to the corresponding public network node; (e) waiting for a return packet from the public network, responsive to the data packet having the replaced source information; (f) replacing, in the return packet, the destination address with the maintained source address; and (g) routing from the filter node, in the private network, the return packet having the replaced destination address to the corresponding private network

20 node.

25

According to a third exemplary aspect, the invention provides a method of operating a filter node for interfacing first and second data communications networks, comprising the steps of: receiving from the first network,

30 a data packet having destination information, which includes a destination address and a destination port, corresponding to a node in the second network and having source information, which includes a source address and a source port, corresponding to a node in the first network;

35 maintaining the source information taken from the data packet in correlation with a unique value representing a port of the filter node; replacing in the data packet the

- 3 -

source address with an address of the filter node and the source port with the filter node port value; and sending to the second network the data packet having the replaced source information, whereby that packet is routed according  
5 to its destination information to the corresponding second network node.

According to a fourth exemplary aspect, the invention provides a filter node for interfacing first and second data communications networks, comprising: means for  
10 receiving from the first network, a data packet having destination information, which includes a destination address and a destination port, corresponding to a node in the public network and having source information, which includes a source address and a source port, corresponding  
15 to a node in the first network; means for maintaining the source information taken from the data packet in correlation with a unique value representing a port of the filter node; means for replacing in the data packet the source address with an address of the filter node and the  
20 source port with the filter node port value; and means for sending to the second network, the data packet having the replaced source information, whereby that packet is routed according to its destination information to the corresponding second network node.

25 An IP filter, embodying the present invention, is a communications device designed to provide public network or Internet access to nodes of private networks, advantageously without requiring the private nodes on such networks to register public Internet addresses. The IP  
30 filter presents a single IP address to the Internet and uses a plurality of IP ports to solve the problem of IP address conservation. It initiates sessions by assigning private side IP sessions to a unique port of the IP filter's public address whereby up to 64,512 (= 65,536  
35 total - 1,024 well known ports) concurrent sessions may be supported through the single IP address. The IP filter effects a translation between a source port number for the

- 4 -

private network and a destination port number for the public network for communication therebetween. Benefits of the IP filter include private node security and conservation of Internet-registered addresses.

5        In a particular embodiment, the IP filter may support three data transport protocols over the internet protocol: transmission control protocol (TCP), user datagram protocol (UDP) and Internet control message protocol (ICMP). Packets of other protocols may be  
10      ignored.

15      The TCP protocol prepends a TCP header to a data packet. The source port and destination port numbers are contained in this header. The Internet addresses of the source and destination nodes are contained in the IP header. The IP address and port information extracted from each packet will be used to determine where the IP filter should route this packet.

20      The IP filter maintains a lookup table of information on each TCP connection. This information includes the port from the private node, the private IP address, the assigned port number of the destination node, and the port number of the IP filter in the form of an index. When a packet is received from the private network, the private address and port number are added to the table  
25      as a new entry, if an entry corresponding to this packet is not found in the table and if the TCP header indicates that this is a new connection request. Then the source address and port number in the packet header are replaced with the IP filter's IP address and port number, and the packet is  
30      transmitted to the Internet.

35      When the IP filter receives a packet from the Internet, the destination port number is used to index the lookup table. When the corresponding table entry is found, the destination address and port number are replaced with the private network's IP address and port number, and the packet is transmitted to the private network. If the received packet's source port is different from the port

- 5 -

recorded in the table, and if the packet header information indicates that this packet is the first response on the connection, then the lookup table is updated with the port number assigned by the Internet node, if needed. When the 5 IP filter detects an end of transmission code in the packet, the lookup table entry is zeroed. If the IP filter receives packets from the Internet that do not have entries in the lookup table corresponding to the IP filter port, it ignores the packets.

10 The UDP protocol is connectionless, as opposed to TCP, a connection-oriented protocol. The UDP header contains no codes governing initial connection or end of transmission. The data of interest in the UDP header are the source port and destination port. This information, 15 along with the Internet addresses contained in the IP header, are used to determine where the IP filter should route this packet.

20 The IP filter maintains a lookup table of information on each UDP session. When the IP filter receives a UDP packet from the private network, it records the source address, the source port number, the destination port number, and the assigned IP filter port number as the index to the table. Then the private node address and port number in the packet header are replaced with the address 25 and assigned port number of the IP filter. Then the packet is transmitted to the Internet.

When the IP filter receives a UDP packet from the Internet, it indexes the UDP lookup table and replaces the packet's destination information, namely the IP filter 30 address and assigned port number, with the private address and port number from the lookup table. The lookup table also maintains an interval indication for an expiration timer on datagram packets received as per standard UDP implementations. If the IP filter receives packets from 35 the Internet that do not have entries in the lookup table corresponding to the IP filter port, it ignores the packets.

- 6 -

As ICMP packets do not contain port numbers of either source or destination, any ICMP packets received from the private network are processed one at a time, with buffering of additional ICMP packets. The IP filter reads 5 the private address from the packet header and replaces it with the address of the IP filter. The packet is transmitted to the Internet, and the IP filter waits for the response. When it receives the responding packet, the destination address in the packet header is changed from 10 that of the IP filter to that of the node on the private network. Then the IP filter transmits the packet to the private network.

To successfully deliver packets over an IP protocol network, each node must maintain a table of other 15 hosts' IP addresses and their corresponding Ethernet addresses in an Ethernet based data communications network. The nodes actually use the IP addresses and the Ethernet addresses to address packets. The relationship between the two addresses is dynamic; that is, a node with an IP 20 address may change its Ethernet address. The information in the address table is obtained from the replies to the node's broadcast of ARP packets. The source node broadcasts ARP packets to request the Ethernet address of the destination node, given the destination node's IP 25 address. If the destination node receives the packet, it sends a reply packet with the requested information.

Though it does not maintain a true ARP table, the IP filter passes ARP packets in a manner similar to TCP and UDP packet passing. When the IP filter receives an ARP 30 packet from a node on the private network destined for the public network, it replaces the source address information with the filter's address information. The private node's IP address and the target IP address are placed in a lookup table. When the target node replies with its own Ethernet 35 address, the destination address information is changed from that of the IP filter to that of the private node before transmitting the packet to the private node. The

- 7 -

private node address information is obtained from the table. When an ARP packet is destined for the firewall, the ARP packet does not pass through the IP filter but is restricted to communications between the filter and the one 5 side of the network.

Events and errors encountered by the IP filter may be logged, for example, by writing them into a text file.

The IP filter ideally will process packets as fast as the networks present them but when network traffic is 10 too heavy, the IP filter will then buffer the packets in two queues, one for the private network and one for the Internet.

Two source and destination lookup tables may be utilized, one for TCP packets and the other for UDP 15 packets. Each table is directly indexed by the IP filter port number assigned to the communication session. The table entries contain the IP address of the private node, the source port of the private node, and the destination port of the Internet node. If there is no connection on a 20 certain IP filter port, then the corresponding entry in the table may be zeroed. Packets arriving from both the private network and the Internet are processed using the same lookup table. This arrangement assumes that of the available IP filter communications ports some are 25 designated for UDP communication and some for TCP communication.

#### Brief Description Of The Drawings

The invention will be better understood from the following description together with reference to the 30 accompanying drawings, in which:

Figure 1 is a schematic representing an internet protocol filter coupling a private network and a public network; and

Figure 2 is a block diagram representing internal 35 components of the filter.

#### Detailed Description

Referring to Figure 1, shown for illustration of

- 8 -

the present invention is a private network 10 communicatively coupled through an internet protocol (IP) filter 12 to a public network 14 which may form part of a global data network, otherwise referred to as the Internet

5 16. The private network 10 represents a conventional data communications network, such as a local area network (LAN), having a plurality of nodes 18 each being identified by a unique IP address within the domain of the private network 10. The public network 14 and Internet 16 are

10 representative of public domain data communications networks also having a plurality of nodes 20 with corresponding IP addresses.

The IP filter 12 acts as a gateway through which data packets are exchanged between the private network 10 and the public network 14, thereby providing Internet access to the nodes 18 of the private network 10. The IP filter 12 constitutes one of the private network nodes 18 and is the only such node to have a public IP address that is Internet-registered, whereby the IP filter 12

15 20 essentially also constitutes one of the public nodes 20 and its IP address is known in the public domain. The IP addresses of the other private network nodes 18 are reserved for the private network 10, and not known or registered in the public Internet address domain. As is conventional, associated with the IP address of the IP filter 12 are a plurality of IP ports, specifically 65,536 in total of which 64,512 are not reserved for predefined

25 30 protocols and can be used for address translations.

Communications between nodes 18 on the private network 10 are unaffected by the presence of the IP filter 12, but to access the public network 14 and particularly the nodes 20 therein, the private nodes 18 route all communications requests through the IP filter 12. The IP filter 12 manages the communications between private nodes

35 40 45 50 55 60 65 70 75 80 85 90 95 100 105 110 115 120 125 130 135 140 145 150 155 160 165 170 175 180 185 190 195 200 205 210 215 220 225 230 235 240 245 250 255 260 265 270 275 280 285 290 295 300 305 310 315 320 325 330 335 340 345 350 355 360 365 370 375 380 385 390 395 400 405 410 415 420 425 430 435 440 445 450 455 460 465 470 475 480 485 490 495 500 505 510 515 520 525 530 535 540 545 550 555 560 565 570 575 580 585 590 595 600 605 610 615 620 625 630 635 640 645 650 655 660 665 670 675 680 685 690 695 700 705 710 715 720 725 730 735 740 745 750 755 760 765 770 775 780 785 790 795 800 805 810 815 820 825 830 835 840 845 850 855 860 865 870 875 880 885 890 895 900 905 910 915 920 925 930 935 940 945 950 955 960 965 970 975 980 985 990 995 1000 1005 1010 1015 1020 1025 1030 1035 1040 1045 1050 1055 1060 1065 1070 1075 1080 1085 1090 1095 1100 1105 1110 1115 1120 1125 1130 1135 1140 1145 1150 1155 1160 1165 1170 1175 1180 1185 1190 1195 1200 1205 1210 1215 1220 1225 1230 1235 1240 1245 1250 1255 1260 1265 1270 1275 1280 1285 1290 1295 1300 1305 1310 1315 1320 1325 1330 1335 1340 1345 1350 1355 1360 1365 1370 1375 1380 1385 1390 1395 1400 1405 1410 1415 1420 1425 1430 1435 1440 1445 1450 1455 1460 1465 1470 1475 1480 1485 1490 1495 1500 1505 1510 1515 1520 1525 1530 1535 1540 1545 1550 1555 1560 1565 1570 1575 1580 1585 1590 1595 1600 1605 1610 1615 1620 1625 1630 1635 1640 1645 1650 1655 1660 1665 1670 1675 1680 1685 1690 1695 1700 1705 1710 1715 1720 1725 1730 1735 1740 1745 1750 1755 1760 1765 1770 1775 1780 1785 1790 1795 1800 1805 1810 1815 1820 1825 1830 1835 1840 1845 1850 1855 1860 1865 1870 1875 1880 1885 1890 1895 1900 1905 1910 1915 1920 1925 1930 1935 1940 1945 1950 1955 1960 1965 1970 1975 1980 1985 1990 1995 2000 2005 2010 2015 2020 2025 2030 2035 2040 2045 2050 2055 2060 2065 2070 2075 2080 2085 2090 2095 2100 2105 2110 2115 2120 2125 2130 2135 2140 2145 2150 2155 2160 2165 2170 2175 2180 2185 2190 2195 2200 2205 2210 2215 2220 2225 2230 2235 2240 2245 2250 2255 2260 2265 2270 2275 2280 2285 2290 2295 2300 2305 2310 2315 2320 2325 2330 2335 2340 2345 2350 2355 2360 2365 2370 2375 2380 2385 2390 2395 2400 2405 2410 2415 2420 2425 2430 2435 2440 2445 2450 2455 2460 2465 2470 2475 2480 2485 2490 2495 2500 2505 2510 2515 2520 2525 2530 2535 2540 2545 2550 2555 2560 2565 2570 2575 2580 2585 2590 2595 2600 2605 2610 2615 2620 2625 2630 2635 2640 2645 2650 2655 2660 2665 2670 2675 2680 2685 2690 2695 2700 2705 2710 2715 2720 2725 2730 2735 2740 2745 2750 2755 2760 2765 2770 2775 2780 2785 2790 2795 2800 2805 2810 2815 2820 2825 2830 2835 2840 2845 2850 2855 2860 2865 2870 2875 2880 2885 2890 2895 2900 2905 2910 2915 2920 2925 2930 2935 2940 2945 2950 2955 2960 2965 2970 2975 2980 2985 2990 2995 3000 3005 3010 3015 3020 3025 3030 3035 3040 3045 3050 3055 3060 3065 3070 3075 3080 3085 3090 3095 3100 3105 3110 3115 3120 3125 3130 3135 3140 3145 3150 3155 3160 3165 3170 3175 3180 3185 3190 3195 3200 3205 3210 3215 3220 3225 3230 3235 3240 3245 3250 3255 3260 3265 3270 3275 3280 3285 3290 3295 3300 3305 3310 3315 3320 3325 3330 3335 3340 3345 3350 3355 3360 3365 3370 3375 3380 3385 3390 3395 3400 3405 3410 3415 3420 3425 3430 3435 3440 3445 3450 3455 3460 3465 3470 3475 3480 3485 3490 3495 3500 3505 3510 3515 3520 3525 3530 3535 3540 3545 3550 3555 3560 3565 3570 3575 3580 3585 3590 3595 3600 3605 3610 3615 3620 3625 3630 3635 3640 3645 3650 3655 3660 3665 3670 3675 3680 3685 3690 3695 3700 3705 3710 3715 3720 3725 3730 3735 3740 3745 3750 3755 3760 3765 3770 3775 3780 3785 3790 3795 3800 3805 3810 3815 3820 3825 3830 3835 3840 3845 3850 3855 3860 3865 3870 3875 3880 3885 3890 3895 3900 3905 3910 3915 3920 3925 3930 3935 3940 3945 3950 3955 3960 3965 3970 3975 3980 3985 3990 3995 4000 4005 4010 4015 4020 4025 4030 4035 4040 4045 4050 4055 4060 4065 4070 4075 4080 4085 4090 4095 4100 4105 4110 4115 4120 4125 4130 4135 4140 4145 4150 4155 4160 4165 4170 4175 4180 4185 4190 4195 4200 4205 4210 4215 4220 4225 4230 4235 4240 4245 4250 4255 4260 4265 4270 4275 4280 4285 4290 4295 4300 4305 4310 4315 4320 4325 4330 4335 4340 4345 4350 4355 4360 4365 4370 4375 4380 4385 4390 4395 4400 4405 4410 4415 4420 4425 4430 4435 4440 4445 4450 4455 4460 4465 4470 4475 4480 4485 4490 4495 4500 4505 4510 4515 4520 4525 4530 4535 4540 4545 4550 4555 4560 4565 4570 4575 4580 4585 4590 4595 4600 4605 4610 4615 4620 4625 4630 4635 4640 4645 4650 4655 4660 4665 4670 4675 4680 4685 4690 4695 4700 4705 4710 4715 4720 4725 4730 4735 4740 4745 4750 4755 4760 4765 4770 4775 4780 4785 4790 4795 4800 4805 4810 4815 4820 4825 4830 4835 4840 4845 4850 4855 4860 4865 4870 4875 4880 4885 4890 4895 4900 4905 4910 4915 4920 4925 4930 4935 4940 4945 4950 4955 4960 4965 4970 4975 4980 4985 4990 4995 5000 5005 5010 5015 5020 5025 5030 5035 5040 5045 5050 5055 5060 5065 5070 5075 5080 5085 5090 5095 5100 5105 5110 5115 5120 5125 5130 5135 5140 5145 5150 5155 5160 5165 5170 5175 5180 5185 5190 5195 5200 5205 5210 5215 5220 5225 5230 5235 5240 5245 5250 5255 5260 5265 5270 5275 5280 5285 5290 5295 5300 5305 5310 5315 5320 5325 5330 5335 5340 5345 5350 5355 5360 5365 5370 5375 5380 5385 5390 5395 5400 5405 5410 5415 5420 5425 5430 5435 5440 5445 5450 5455 5460 5465 5470 5475 5480 5485 5490 5495 5500 5505 5510 5515 5520 5525 5530 5535 5540 5545 5550 5555 5560 5565 5570 5575 5580 5585 5590 5595 5600 5605 5610 5615 5620 5625 5630 5635 5640 5645 5650 5655 5660 5665 5670 5675 5680 5685 5690 5695 5700 5705 5710 5715 5720 5725 5730 5735 5740 5745 5750 5755 5760 5765 5770 5775 5780 5785 5790 5795 5800 5805 5810 5815 5820 5825 5830 5835 5840 5845 5850 5855 5860 5865 5870 5875 5880 5885 5890 5895 5900 5905 5910 5915 5920 5925 5930 5935 5940 5945 5950 5955 5960 5965 5970 5975 5980 5985 5990 5995 6000 6005 6010 6015 6020 6025 6030 6035 6040 6045 6050 6055 6060 6065 6070 6075 6080 6085 6090 6095 6100 6105 6110 6115 6120 6125 6130 6135 6140 6145 6150 6155 6160 6165 6170 6175 6180 6185 6190 6195 6200 6205 6210 6215 6220 6225 6230 6235 6240 6245 6250 6255 6260 6265 6270 6275 6280 6285 6290 6295 6300 6305 6310 6315 6320 6325 6330 6335 6340 6345 6350 6355 6360 6365 6370 6375 6380 6385 6390 6395 6400 6405 6410 6415 6420 6425 6430 6435 6440 6445 6450 6455 6460 6465 6470 6475 6480 6485 6490 6495 6500 6505 6510 6515 6520 6525 6530 6535 6540 6545 6550 6555 6560 6565 6570 6575 6580 6585 6590 6595 6600 6605 6610 6615 6620 6625 6630 6635 6640 6645 6650 6655 6660 6665 6670 6675 6680 6685 6690 6695 6700 6705 6710 6715 6720 6725 6730 6735 6740 6745 6750 6755 6760 6765 6770 6775 6780 6785 6790 6795 6800 6805 6810 6815 6820 6825 6830 6835 6840 6845 6850 6855 6860 6865 6870 6875 6880 6885 6890 6895 6900 6905 6910 6915 6920 6925 6930 6935 6940 6945 6950 6955 6960 6965 6970 6975 6980 6985 6990 6995 7000 7005 7010 7015 7020 7025 7030 7035 7040 7045 7050 7055 7060 7065 7070 7075 7080 7085 7090 7095 7100 7105 7110 7115 7120 7125 7130 7135 7140 7145 7150 7155 7160 7165 7170 7175 7180 7185 7190 7195 7200 7205 7210 7215 7220 7225 7230 7235 7240 7245 7250 7255 7260 7265 7270 7275 7280 7285 7290 7295 7300 7305 7310 7315 7320 7325 7330 7335 7340 7345 7350 7355 7360 7365 7370 7375 7380 7385 7390 7395 7400 7405 7410 7415 7420 7425 7430 7435 7440 7445 7450 7455 7460 7465 7470 7475 7480 7485 7490 7495 7500 7505 7510 7515 7520 7525 7530 7535 7540 7545 7550 7555 7560 7565 7570 7575 7580 7585 7590 7595 7600 7605 7610 7615 7620 7625 7630 7635 7640 7645 7650 7655 7660 7665 7670 7675 7680 7685 7690 7695 7700 7705 7710 7715 7720 7725 7730 7735 7740 7745 7750 7755 7760 7765 7770 7775 7780 7785 7790 7795 7800 7805 7810 7815 7820 7825 7830 7835 7840 7845 7850 7855 7860 7865 7870 7875 7880 7885 7890 7895 7900 7905 7910 7915 7920 7925 7930 7935 7940 7945 7950 7955 7960 7965 7970 7975 7980 7985 7990 7995 8000 8005 8010 8015 8020 8025 8030 8035 8040 8045 8050 8055 8060 8065 8070 8075 8080 8085 8090 8095 8100 8105 8110 8115 8120 8125 8130 8135 8140 8145 8150 8155 8160 8165 8170 8175 8180 8185 8190 8195 8200 8205 8210 8215 8220 8225 8230 8235 8240 8245 8250 8255 8260 8265 8270 8275 8280 8285 8290 8295 8300 8305 8310 8315 8320 8325 8330 8335 8340 8345 8350 8355 8360 8365 8370 8375 8380 8385 8390 8395 8400 8405 8410 8415 8420 8425 8430 8435 8440 8445 8450 8455 8460 8465 8470 8475 8480 8485 8490 8495 8500 8505 8510 8515 8520 8525 8530 8535 8540 8545 8550 8555 8560 8565 8570 8575 8580 8585 8590 8595 8600 8605 8610 8615 8620 8625 8630 8635 8640 8645 8650 8655 8660 8665 8670 8675 8680 8685 8690 8695 8700 8705 8710 8715 8720 8725 8730 8735 8740 8745 8750 8755 8760 8765 8770 8775 8780 8785 8790 8795 8800 8805 8810 8815 8820 8825 8830 8835 8840 8845 8850 8855 8860 8865 8870 8875 8880 8885 8890 8895 8900 8905 8910 8915 8920 8925 8930 8935 8940 8945 8950 8955 8960 8965 8970 8975 8980 8985 8990 8995 9000 9005 9010 9015 9020 9025 9030 9035 9040 9045 9050 9055 9060 9065 9070 9075 9080 9085 9090 9095 9100 9105 9110 9115 9120 9125 9130 9135 9140 9145 9150 9155 9160 9165 9170 9175 9180 9185 9190 9195 9200 9205 9210 9215 9220 9225 9230 9235 9240 9245 9250 9255 9260 9265 9270 9275 9280 9285 9290 9295 9300 9305 9310 9315 9320 9325 9330 9335 9340 9345 9350 9355 9360 9365 9370 9375 9380 9385 9390 9395 9400 9405 9410 9415 9420 9425 9430 9435 9440 9445 9450 9455 9460 9465 9470 9475 9480 9485 9490 9495 9500 9505 9510 9515 9520 9525 9530 9535 9540 9545 9550 9555 9560 9565 9570 9575 9580 9585 9590 9595 9600 9605 9610 9615 9620 9625 9630 9635 9640 9645 9650 9655 9660 9665 9670 9675 9680 9685 9690 9695 9700 9705 9710 9715 9720 9725 9730 9735 9740 9745 9750 9755 9760 9765 9770 9775 9780 9785 9790 9795 9800 9805 9810 9815 9820 9825 9830 9835 9840 9845 9850 9855 9860 9865 9870 9875 9880 9885 9890 9895 9900 9905 9910 9915 9920 9925 9930 9935 9940 9945 9950 9955 9960 9965 9970 9975 9980 9985 9990 9995 9999

- 9 -

14. The modifications cause the communications between the private nodes 18 and the public Internet nodes 20 to actually be between the IP filter 12 and the Internet nodes 20, which route all return communications to the IP filter 5 12 which subsequently routes the return data packets to the private nodes 18.

The IP filter 12 accepts no connection requests from the public network 14. All communications between private nodes 18 and public nodes 20 are initiated by the 10 private nodes 18. The IP filter 12 is designed to support three data transport protocols over the internet protocol: TCP, UDP and ICMP messages; packets of other protocols are rejected or ignored.

A translation table is maintained by the IP filter 15 12 to map address and ports for packets received from the private network 10 destined to the public network 14 and vise versa. The translation table contains the following for each entry:

|    |                              |         |
|----|------------------------------|---------|
| 20 | private IP address           | (pIP)   |
|    | private port                 | (pPort) |
|    | internet (public) IP address | (iIP)   |
|    | internet (public) Port       | (iPort) |
|    | timer                        |         |
|    | session type/state           |         |
| 25 | Ethernet address             |         |

The basic translation substitutes IP addresses and ports from the private network side to the IP filter's IP address and ports, thereby hiding all nodes 18 on the private network 10 from the public network 14.

30 A packet originating on the private network side specifies a source - destination of  
(pIP, pPort - iIP, iPort)

This defines a "socket" in which the endpoints of the connection (source and destination) are defined by the IP 35 addresses in the IP header and the ports in the TCP or UDP header.

The IP filter 12 will translate the above to

- 10 -

(frIP, frPort - iIP, iPort)

where frIP is the IP address of the IP filter 12 on the public network 14, and frPort is the index into the translation table plus an offset value, for example, of 5 1024 to skip using well known ports. The frPort represents an arbitrary port.

The internet node 20 will reply with a packet

(iIP, iPort - frIP, frPort)

which will be received by the IP filter 12 and translated 10 thereby to

(iIP, iPort - pIP, pPort)

In general, to translate from the private side, the values (protocol type, pIP, pPort, iIP, iPort) must be located in the translation table. This should be done with 15 a hash table lookup.

Translating from the public side can be a direct table lookup since frPort minus 1024 is the index into the table. If (iIP, iPort) in the packet does not match the corresponding entries in the table, then an unauthorized 20 access is logged and the packet dropped.

In translating packets, when a port is substituted in the TCP or UDP header, the checksum in both the TCP/UCP and IP header must be recalculated. When an IP address is substituted in the IP header, the IP header checksum must 25 be recalculated.

Following are special considerations for different protocols supported by the IP filter 12.

In respect of TCP, when a SYN packet is received from the private network 10, the IP filter 12 locates an 30 unused entry in the table and fills it in, setting the type to TCP and state to SYN. Then the packet is forwarded by the general scheme above. If no free entries exist in the table, then the packet is dropped and the event is logged.

If a SYN packet is received from the public 35 network 14 interface, it is treated as unauthorized and logged (except for FTP special case described below). However, a SYN+ACK packet is forwarded if the state of the

- 11 -

translation table entry is SYN. After forwarding such a packet the state set to OPEN.

If a FIN packet is received by the IP filter 12 and if the state in the translation table is not FIN, the 5 state is set to FIN and the packet forwarded. If the state is FIN, then the packet is forwarded and the translation table entry is deleted by setting it to 0. A FIN must be sent by each side to close a TCP connection.

If a RST packet is received, then the translation 10 table entry is deleted.

Having regard now to the UDP protocol, when any UDP packet is received from the private network 10 side, the IP filter 12 first tries its standard lookup. If a translation table entry is not found, an unused entry is 15 set up and the state set to OPEN. If a free entry is not found in the table, then rather than dropping the packet, a random UDP in the table is overwritten. Since UDP is connectionless and consequently an unreliable transport, if a packet is received from the public network 14 that would 20 have needed the entry that was overwritten, that packet will be dropped and the node 18 on the private side will need to retry.

With regard to FTP, an FTP client establishes a TCP "control" connection with an FTP server on a particular 25 port, for example, port 21. However, when data is to be transmitted, the FTP server will open a TCP connection from its "data" port, for example, which is default 20, to a destination port specified by the client.

To support this, packets sent by the private 30 network 10 to port 21 need to be analyzed for an FTP "port" command at the IP filter 12. If detected, then a new entry in the table must be set up with pPort set to the value in the FTP port command. The IP address and port number in the FTP command must be changed to the IP filter's address 35 and port before forwarding the packet. The state is set to FTPDATA.

When a SYN packet is received from the public

- 12 -

network 14, if a table entry exists and is in FTPDATA state, then the packet is forwarded and the state set to OPEN.

For the ICMP protocol, if an ICMP packet is received from the private network 10 and if that packet is an echo request (ping), then the IP filter 12 locates a new entry in the translation table. The sequence field of the packet is stored in pPort in the table and the table index is put in the sequence field of the packet. The ICMP checksum is recalculated and the standard IP header substitution is done. The type is set to ICMP and state to PING and the timer set to 1 minute.

If an echo reply (ping) is received from the public network 14 interface, then the sequence field is used as the index into the table. If the state is PING, then pPort in the table is substituted into the sequence field of the packet, the ICMP checksum recalculated and the standard IP header substitution is done. The table entry is then deleted.

If an echo request (ping) is received from the public network 14, then the IP filter 12 will reply. This allows internet access to confirm that the IP filter 12 is reachable and running.

If a Destination Unreachable packet is received from the public network 14, then the header information contained is extracted. If the protocol was TCP or UDP, the (frIP, frPort - iIP, iPort) of the originating packet can be determined and the translation table entry located. If the IP address extracted from the ICMP matches the address in the table, the IP filter 12 forwards the packet to the private network 10 using the standard scheme.

All other ICMP packets received from either side are dropped and logged.

Since most data communications protocols are based on either the UDP or TCP protocols, these other protocols are compatible with the IP filter 12 as long as they do not initiate negotiations like FTP to have the server open a

- 13 -

connection back to the client. Examples of other compatible protocols include: Telnet; TFTP (Trivial File Transfer Protocol); DNS (Domain Name Services); and Web browsers.

5 Whenever a packet is transmitted in either direction, the timer field of the translation table entry is set to the configured timeout value (except ping). Each minute, the timer field of all active entries in the tables are decremented and if they become 0, then the translation  
10 table entry is deleted. This will clear out UDP and PING entries which are no longer in use and also TCP entries which have had an abnormal termination and did not send FIN from each side. It could be a security hole to leave an unused entry in the table for too long. A good timeout  
15 value to be configured would be just longer than the typical TCP keep alive.

According to a particular embodiment, the private network 10 and the public network 14 are Ethernet based LANs. The IP filter 12 may be implemented by a data  
20 processing platform which is equipped with two conventional Ethernet hardware interfaces connected to networks 10 and 14, respectively, and which is provisioned with appropriate software to implement the functionality of the IP filter 12.

25 Internal components of the IP filter 12 in terms of software executable by the data processing platform are shown in Figure 2. The internal components include two packet drivers 30 and 32, an address resolution protocol (ARP) table 34, an Ethernet address table 36, an IP handler  
30 38, an address translation 40 and a user interface 42. The packet drivers 30 and 32 control the Ethernet hardware interfaces in order to communicate with, respectively, the private network 10 and the public network 14. The IP  
35 handler 38 provides a router functionality for receiving and forwarding messages, and maintains the ARP table 34 and the Ethernet table 36. The address translation 40 effects translation between source port numbers from the private

- 14 -

network 10 and the destination port numbers on the public network side 14. The user interface 42 enables an operator, via a keyboard and display terminal attached to the processing platform, to interface with the IP filter 12. Functions keys are provided to configure the IP filter, view or copy log files, display status, etc. The log file will contain the connect time of TCP or UDP sessions, inbound and outbound traffic statistics, and invalid access to the IP filter 12. To prevent the log file from growing too large, this information will be logged to a new file when the date changes.

Routing of packets to and from the IP filter 12 is described in the following in terms of a public interface, from the view of the public network 14, and of a private interface, from the view of the private network 10.

The public interface behaves as a host on the LAN segment. To forward a packet, it checks to see if the destination IP is on the local LAN segment. If it is, it looks up the IP address in its ARP table to find the Ethernet address. If there is no entry in the ARP table, it must put the packet on a queue and send out an ARP request to get the Ethernet address. Standard aging out of ARP table entries needs to be done. If the IP destination is not on the LAN segment, it will forward the packet to the configured default router. ICMP Redirect messages sent by the default router will be ignored.

The private interface effects the functionality of a router, as it needs to be able to forward packets to one or more routers to communicate with the remote client stations. A large remote client network may access multiple router machines. Conventional routing can result in large routing tables because the routing entries become host addresses instead of subnet addresses. That is, if the network is set up so that a client may come in through either Router1 or Router2, then no single router can be the router for the subnet that that client station is on. A conventional router that would get routing tables via RIP

- 15 -

from all routers on the private network would end up with a large table of host addresses for each remote client connected. This can affect performance in the search time necessary to find the route, the memory required for large 5 tables and the amount of RIP traffic on the LAN segment between all these routers.

To handle routing in this environment, the IP filter will maintain an Ethernet table. For every packet that is forwarded from the private to public side, if a 10 translation entry exists, use its Ethernet index to compare with the Ethernet source address of the incoming packet. If they match, nothing more needs to be done. Otherwise, the Ethernet table is searched for the source Ethernet address, adding a new Ethernet table entry if not found. 15 The index to the Ethernet table is then saved in the translation table entry. Then when a packet is being translated from the public to private side, the Ethernet address can be retrieved directly from the index in the translation table. Thus packets will be routed to the 20 router which forwarded the packet to the IP filter.

Those skilled in the art will recognize that various modifications and changes could be made to the invention without departing from the spirit and scope thereof. It should therefore be understood that the claims 25 are not to be considered as being limited to the precise embodiments set forth above, in the absence of specific limitations directed to each embodiment.

- 16 -

WE CLAIM:

1. A method of interfacing private (10) and public (14) data communications networks, through a filter node (12) in communication with both networks, the filter node 5 having an address known in the public network, comprising the steps of:

routing from nodes (18) in the private network, to the filter node, data packets having destination information, which includes a destination address and a 10 destination port, corresponding to nodes (20) in the public network and having source information, which includes a source address and a source port, of the respective private network nodes;

15 for each data packet received from the private network, at the filter node, maintaining the source information taken from the data packet in correlation with a unique value representing a port of the filter node, and replacing in the data packet the source address with the filter node address and the source port with the filter 20 node port value; and

routing from the filter node, in the public network, the data packets having the replaced source information, according to the destination information in each, to the corresponding public network nodes.

25 2. A method as claimed in claim 1, comprising the steps of:

routing from nodes in the public network, to the filter node, data packets each having the address of the 30 filter node as the destination address;

for each data packet received from the public network, at the filter node, correlating the destination port of the destination information in the data packet to particular source information being maintained and 35 replacing, in the data packet, the destination information with the particular source information;

routing from the filter node, in the private

network, the data packets having the replaced destination information to the corresponding private network nodes.

3. A method as claimed in claim 2, comprising  
5 ignoring by the filter node a data packet received from the public network, if the destination port of the destination information in that data packet can not be correlated to the maintained source information.

10 4. A method as claimed in claim 3, wherein  
maintaining the source information includes storing the source information from each data packet as an entry in a lookup table, and the filter node port value correlating to the source information constitutes an index into the table  
15 for that entry.

5. A method as claimed in claim 4, wherein the data packets include packets in accordance with a transmission control protocol (TCP) over an internet protocol (IP).

20 6. A method as claimed in claim 5, comprising  
receiving at the filter node a TCP packet from the private network; and if an entry corresponding to the TCP packet is not found in the lookup table and the TCP packet indicates  
25 that this is a connection request, storing the source information together with the destination information from the TCP packet as a new entry in the lookup table.

7. A method as claimed in claim 6, comprising  
30 receiving at the filter node a TCP packet from the public network; and if the source port in the received TCP packet is different from the destination port in a source information entry of the lookup table, indexed by the destination port in the TCP packet, and if the TCP packet  
35 indicates that this packet is a first response to the connection request, then updating by the filter node the destination port in the table entry with the source port

- 18 -

from the received TCP packet.

8. A method as claimed in claim 7, comprising receiving at the filter node a TCP packet having an end of 5 transmission code in the packet and zeroing an entry in the lookup table corresponding to the received TCP packet.

9. A method as claimed in claim 4, wherein the data 10 packets include packets in accordance with a user datagram protocol (UDP) over an internet protocol (IP).

10. A method as claimed in claim 9, comprising receiving at the filter node a UDP data packet from the private network, and adding the source information and the 15 destination information from the UDP packet together with an interval indication for an expiration timer as a new entry in the lookup table.

11. A method of interfacing private (10) and public 20 data (14) communications networks, through a filter node (12) in communication with both networks, comprising the steps of:

(a) receiving at the filter node, from the private network, a data packet having an a destination address 25 corresponding to a node (20) in the public network and a source address corresponding to a node (18) in the private network;

(b) maintaining, by the filter node, the source address taken from the data packet;

30 (c) replacing, in the data packet, the source address with an address of the filter node;

(d) routing from the filter node, in the public network, the data packet having the replaced source address, according to the destination address, to the 35 corresponding public network node;

(e) waiting for a return packet from the public network, responsive to the data packet having the replaced

source information;

(f) replacing, in the return packet, the destination address with the maintained source address; and

(g) routing from the filter node, in the private

5 network, the return packet having the replaced destination address to the corresponding private network node.

12. A method as claimed in claim 11, comprising buffering, at the filter node, further data packets 10 received from the private network while waiting for the return packet, and repeating steps (b) through (g) on an individual basis for the further packets, if any, that were buffered.

15 13. A method as claimed in claim 12, wherein the data packets include packets in accordance with an internet control message protocol (ICMP).

14. A method of operating a filter node (12) for 20 interfacing first (10) and second (14) data communications networks, comprising the steps of:

receiving from the first network, a data packet having destination information, which includes a destination address and a destination port, corresponding 25 to a node (20) in the second network and having source information, which includes a source address and a source port, corresponding to a node (18) in the first network;

maintaining the source information taken from the data packet in correlation with a unique value representing 30 a port of the filter node;

replacing in the data packet the source address with an address of the filter node and the source port with the filter node port value; and

sending to the second network the data packet 35 having the replaced source information, whereby that packet is routed according to its destination information to the corresponding second network node.

- 20 -

15. A method as claimed in claim 14, comprising the steps of:

receiving from the second network, a data packet 5 having the address of the filter node as the destination address;

correlating the destination port of the destination information in the data packet to particular source information being maintained;

10 replacing, in the data packet, the destination information with the particular source information;

sending to the first network the data packet having the replaced destination information, whereby that packet is routed according to its destination information 15 to the corresponding first network node.

16. A method as claimed in claim 15, comprising ignoring a data packet received from the second network, if 20 the destination port of the destination information in that data packet can not be correlated to the maintained source information.

17. A method as claimed in claim 16, wherein maintaining the source information includes storing the 25 source information from the data packet as an entry in a lookup table, and the filter node port value correlating to the source information constitutes an index into the table for that entry.

30 18. A method as claimed in claim 17, wherein the data packets include packets in accordance with a transmission control protocol (TCP) over an internet protocol (IP).

19. A method as claimed in claim 18, comprising 35 receiving a TCP packet from the first network; and if an entry corresponding to the TCP packet is not found in the lookup table and the TCP packet indicates that this is a

- 21 -

connection request, storing the source information together with the destination information from the TCP packet as a new entry in the lookup table.

5 20. A method as claimed in claim 19, comprising receiving a TCP packet from the second network; and if the source port in the received TCP packet is different from the destination port in a source information entry of the lookup table, indexed by the destination port in the TCP 10 packet, and if the TCP packet indicates that this packet is a first response to the connection request, then updating the destination port in the table entry with the source port from the received TCP packet.

15 21. A method as claimed in claim 20, comprising receiving a TCP packet having an end of transmission code in the packet, and zeroing an entry in the lookup table corresponding to the received TCP packet.

20 22. A method as claimed in claim 17, wherein the data packets include packets in accordance with a user datagram protocol (UDP) over an internet protocol (IP).

25 23. A method as claimed in claim 22, comprising receiving a UDP data packet from the first network, and adding the source information and the destination information from the UDP packet together with an interval indication for an expiration timer as a new entry in the lookup table.

30 24. A method of operating a filter node (14) for interfacing first (10) and second (14) data communications networks, comprising the steps of:  
(a) receiving from the first network, a data packet 35 having an a destination address corresponding to a node (20) in the second network and a source address corresponding to a node (18) in the first network;

- 22 -

- (b) maintaining the source address taken from the data packet;
- (c) replacing, in the data packet, the source address with an address of the filter node;
- 5 (d) sending to the second network the data packet having the replaced source address, whereby that packet is routed to the corresponding second network node;
- (e) receiving a return packet from the second network, responsive to the data packet having the replaced source
- 10 information;
- (f) replacing, in the return packet, the destination address with the maintained source address; and
- (g) sending to the first network the return packet having the replaced destination address, whereby that
- 15 packet is routed to the corresponding first network node.

25. A method as claimed in claim 24, comprising buffering further data packets received from the first network while waiting for the return packet, and repeating steps (b) through (g) on an individual basis for the further packets, if any, that were buffered.

26. A method as claimed in claim 25, wherein the data packets include packets in accordance with an internet control message protocol (ICMP).

27. A filter node (12) for interfacing first (10) and second (14) data communications networks, comprising:  
means for receiving from the first network, a data  
30 packet having destination information, which includes a destination address and a destination port, corresponding to a node (20) in the second network and having source information, which includes a source address and a source port, corresponding to a node (18) in the first network;  
35 means for maintaining the source information taken from the data packet in correlation with a unique value representing a port of the filter node;

- 23 -

means for replacing in the data packet the source address with an address of the filter node and the source port with the filter node port value; and

5 means for sending to the second network, the data packet having the replaced source information, whereby that packet is routed according to its destination information to the corresponding second network node.

28. A filter node as claimed in claim 27, comprising:  
10 means for receiving from the second network, a data packet having the address of the filter node as the destination address;

15 means for correlating the destination port of the destination information in the data packet to particular source information being maintained;

means for replacing, in the data packet, the destination information with the particular source information; and

20 means for sending to the first network the data packet having the replaced destination information, whereby that packet is routed according to its destination information to the corresponding first network node.

29. A method as claimed in claim 28, comprising means  
25 for ignoring a data packet received from the second network, if the destination port of the destination information in that data packet can not be correlated to the maintained source information.

30. 30. A method as claimed in claim 29, wherein the means for maintaining the source information includes means for storing the source information from the data packet as an entry in a lookup table, and wherein the filter node port value correlating to the source information constitutes an  
35 index into the table for that entry.

31. A filter node (12) for interfacing first (10) and

- 24 -

second (14) data communications networks, comprising:

(a) means for receiving from the first network, a data packet having an a destination address corresponding to a node (20) in the second network and a source address corresponding to a node (18) in the first network;

5 (b) means for maintaining the source address taken from the data packet;

(c) means for replacing, in the data packet, the source address with an address of the filter node;

10 (d) means for sending to the second network the data packet having the replaced source address, whereby that packet is routed to the corresponding second network node;

(e) means for receiving a return packet from the second network, responsive to the data packet having the replaced source information;

15 (f) means for replacing, in the return packet, the destination address with the maintained source address; and

(g) means for sending to the first network the return packet having the replaced destination address, whereby that packet is routed to the corresponding first network node.

32. A filter node as claimed in claim 31, comprising means for buffering further data packets received from the first network while waiting for the return packet, and means for controlling means (b) through (g) on an individual basis for processing the further packets, if any, that were buffered.

1/2

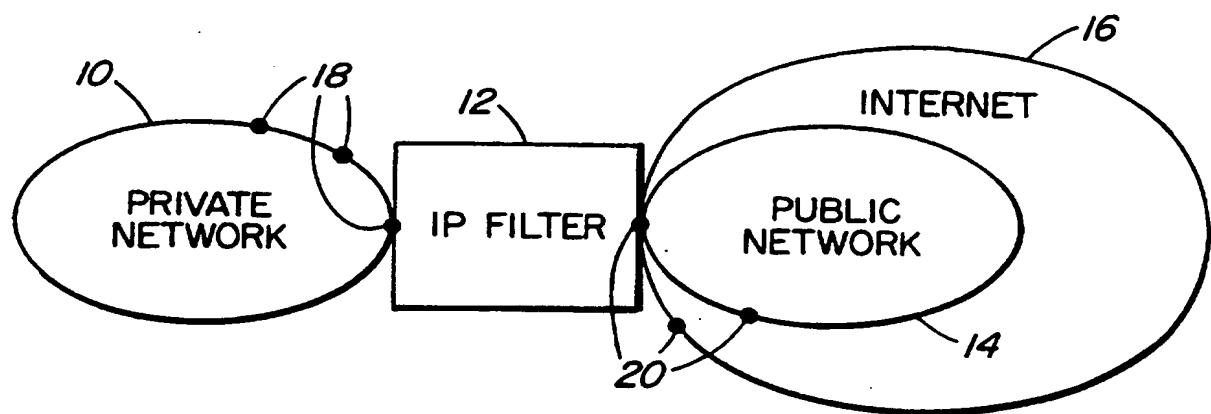


FIG. 1

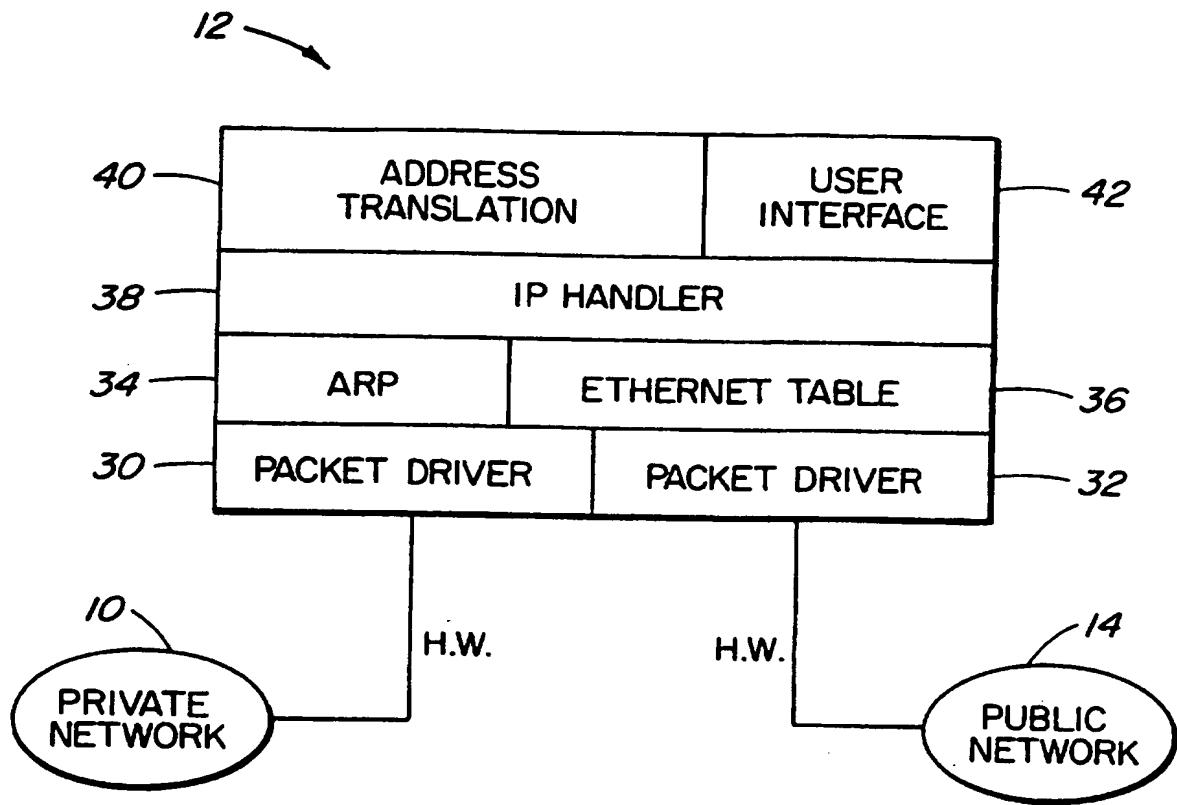


FIG. 2

## INTERNATIONAL SEARCH REPORT

Int'l Application No  
PCT/CA 97/00269A. CLASSIFICATION OF SUBJECT MATTER  
IPC 6 H04L29/06 H04L12/46

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)  
IPC 6 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category | Citation of document, with indication, where appropriate, of the relevant passages   | Relevant to claim No. |
|----------|--|-----------------------|
| A        | RFC1631,<br>May 1994, INTERNET ENGINEERING TASK<br>FORCE, USA,<br>pages 1-10, XP002040992<br>EGEVANG K AND FRANCIS P: "The IP Network<br>Address Translator (NAT)"<br>see paragraph 2; figures 1,2<br>see paragraph 3.3<br>--- | 1,11,14,<br>24,27,31  |
| A        | EP 0 465 201 A (DIGITAL EQUIPMENT CORP) 8<br>January 1992<br>see column 7, line 30 - column 8, line 27<br>see column 10, line 45 - column 12, line<br>22; figure 2<br>---  | 1,11,14,<br>24,27,31  |

 Further documents are listed in the continuation of box C. Patent family members are listed in annex.

## \* Special categories of cited documents :

- \*A\* document defining the general state of the art which is not considered to be of particular relevance
- \*E\* earlier document but published on or after the international filing date
- \*L\* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- \*O\* document referring to an oral disclosure, use, exhibition or other means
- \*P\* document published prior to the international filing date but later than the priority date claimed

- \*T\* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- \*X\* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- \*Y\* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
- \*Z\* document member of the same patent family

11

Date of the actual completion of the international search

19 September 1997

Date of mailing of the international search report

14.10.1997

Name and mailing address of the ISA  
European Patent Office, P.B. 5818 Patentlaan 2  
NL - 2280 HV Rijswijk  
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,  
Fax (+31-70) 340-3016

Authorized officer

Dupuis, H

**INTERNATIONAL SEARCH REPORT**Int'l Application No  
PCT/CA 97/00269**C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT**

| Category * | Citation of document, with indication, where appropriate, of the relevant passages  | Relevant to claim No. |
|------------|---|-----------------------|
| A          | INTERNET SECURITY HANDBOOK,<br>1995, MAIDENHEAD, ENGLAND,<br>pages 27-37, XP002040993<br>STALLINGS W:<br>see page 31; figure 3.2<br>----- | 11,24,31              |

## INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No  
PCT/CA 97/00269

| Patent document cited in search report | Publication date | Patent family member(s)  | Publication date                             |
|--|------------------|--|--|
| EP 0465201 A                           | 08-01-92         | US 5309437 A<br>CA 2044363 A<br>DE 69122439 D<br>DE 69122439 T | 03-05-94<br>30-12-91<br>07-11-96<br>15-05-97 |

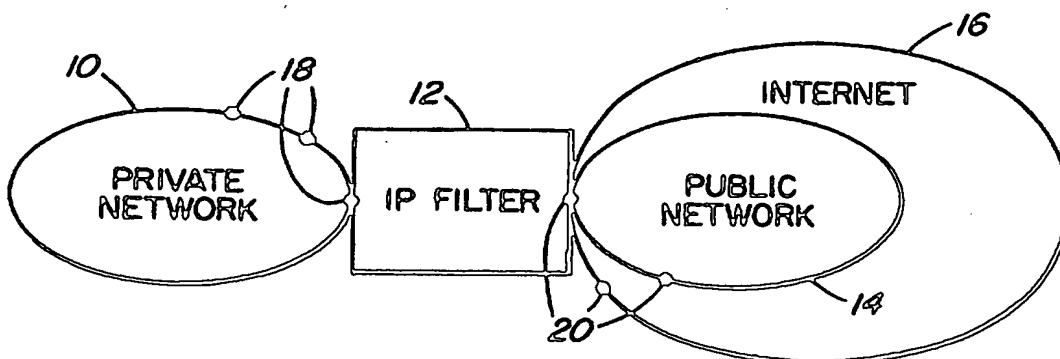
**THIS PAGE BLANK (USPTO)**



## INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

|  |  |  |   |
|--|--|--|---|
| (51) International Patent Classification <sup>6</sup> :<br><br>H04L 29/06, 12/46   |  | A3   | (11) International Publication Number: WO 97/40610<br><br>(43) International Publication Date: 30 October 1997 (30.10.97) |
| (21) International Application Number: PCT/CA97/00269<br><br>(22) International Filing Date: 23 April 1997 (23.04.97)  |  | (81) Designated States: AU, CA, CN, JP, KR, European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).  |   |
| (30) Priority Data:<br>60/015,945 24 April 1996 (24.04.96) US  |  | Published<br><i>With international search report.<br/>Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.</i> |   |
| (71) Applicant: NORTHERN TELECOM LIMITED [CA/CA];<br>World Trade Center of Montreal, 8th floor, 380 St. Antoine Street West, Montreal, Quebec H2Y 3Y4 (CA).  |  | (88) Date of publication of the international search report:<br>27 November 1997 (27.11.97)  |   |
| (72) Inventors: WOOTTON, Bruce, Anthony; 10601 Bent Twig Drive, Raleigh, NC 27613 (US). COLVIN, William, G.; 874 Childs Drive, Milton, Ontario L9T 4J6 (CA). |  |  |   |
| (74) Agent: GRANCHELLI, John, A.; Northern Telecom Limited, Patent Dept., P.O. Box 3511, Station "C", Ottawa, Ontario K1Y 4H7 (CA).                          |  |  |   |

## (54) Title: INTERNET PROTOCOL FILTER



## (57) Abstract

The IP filter (12), embodying the present invention, is a communications device designed to provide public network (14) or Internet (16) access to nodes (18) of private networks (10), advantageously without requiring the private nodes on such networks to register public Internet addresses. The IP filter presents a single IP address to the Internet and uses a plurality of IP ports to solve the problem of IP address conservation. It initiates sessions by assigning private side IP sessions to a unique port of the IP filter's public address. The IP filter effects a translation between a source port number for the private network and a destination port number for the public network for communication therebetween. Benefits of the IP filter include private node security and conservation of Internet-registered addresses.

**FOR THE PURPOSES OF INFORMATION ONLY**

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

|    |                          |    |                                       |    |   |    |                          |
|----|--------------------------|----|---------------------------------------|----|---|----|--------------------------|
| AI | Albania                  | ES | Spain                                 | LS | Lesotho                                   | SI | Slovenia                 |
| AM | Armenia                  | FI | Finland                               | LT | Lithuania                                 | SK | Slovakia                 |
| AT | Austria                  | FR | France                                | LU | Luxembourg                                | SN | Senegal                  |
| AU | Australia                | GA | Gabon                                 | LV | Latvia                                    | SZ | Swaziland                |
| AZ | Azerbaijan               | GB | United Kingdom                        | MC | Monaco                                    | TD | Chad                     |
| BA | Bosnia and Herzegovina   | GE | Georgia                               | MD | Republic of Moldova                       | TG | Togo                     |
| BB | Barbados                 | GH | Ghana                                 | MG | Madagascar                                | TJ | Tajikistan               |
| BE | Belgium                  | GN | Guinea                                | MK | The former Yugoslav Republic of Macedonia | TM | Turkmenistan             |
| BF | Burkina Faso             | GR | Greece                                | ML | Mali                                      | TR | Turkey                   |
| BG | Bulgaria                 | HU | Hungary                               | MN | Mongolia                                  | TT | Trinidad and Tobago      |
| BJ | Benin                    | IE | Ireland                               | MR | Mauritania                                | UA | Ukraine                  |
| BR | Brazil                   | IL | Israel                                | MW | Malawi                                    | UG | Uganda                   |
| BY | Belarus                  | IS | Iceland                               | MX | Mexico                                    | US | United States of America |
| CA | Canada                   | IT | Italy                                 | NE | Niger                                     | UZ | Uzbekistan               |
| CF | Central African Republic | JP | Japan                                 | NL | Netherlands                               | VN | Viet Nam                 |
| CG | Congo                    | KE | Kenya                                 | NO | Norway                                    | YU | Yugoslavia               |
| CH | Switzerland              | KG | Kyrgyzstan                            | NZ | New Zealand                               | ZW | Zimbabwe                 |
| CI | Côte d'Ivoire            | KP | Democratic People's Republic of Korea | PL | Poland                                    |    |                          |
| CM | Cameroon                 | KR | Republic of Korea                     | PT | Portugal                                  |    |                          |
| CN | China                    | KZ | Kazakhstan                            | RO | Romania                                   |    |                          |
| CU | Cuba                     | LC | Saint Lucia                           | RU | Russian Federation                        |    |                          |
| CZ | Czech Republic           | LI | Liechtenstein                         | SD | Sudan                                     |    |                          |
| DE | Germany                  | LK | Sri Lanka                             | SE | Sweden                                    |    |                          |
| DK | Denmark                  | LR | Liberia                               | SG | Singapore                                 |    |                          |
| EE | Estonia                  |    |                                       |    |   |    |                          |

# INTERNATIONAL SEARCH REPORT

Int'l Application No  
PCT/CA 97/00269

**A. CLASSIFICATION OF SUBJECT MATTER**  
IPC 6 H04L29/06 H04L12/46

According to International Patent Classification (IPC) or to both national classification and IPC

**B. FIELDS SEARCHED**

Minimum documentation searched (classification system followed by classification symbols)  
IPC 6 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

| Category | Citation of document, with indication, where appropriate, of the relevant passages  | Relevant to claim No. |
|----------|---|-----------------------|
| A        | RFC1631,<br>May 1994, INTERNET ENGINEERING TASK<br>FORCE, USA,<br>pages 1-10, XP002040992<br>EGEVANG K AND FRANCIS P: "The IP Network<br>Address Translator (NAT)"<br>see paragraph 2; figures 1,2<br>see paragraph 3.3<br>---<br>EP 0 465 201 A (DIGITAL EQUIPMENT CORP) 8<br>January 1992<br>see column 7, line 30 - column 8, line 27<br>see column 10, line 45 - column 12, line<br>22; figure 2<br>---<br>-/-/ | 1,11,14,<br>24,27,31  |
| A        |   | 1,11,14,<br>24,27,31  |

Further documents are listed in the continuation of box C.

Patent family members are listed in annex.

\* Special categories of cited documents :

- \*A\* document defining the general state of the art which is not considered to be of particular relevance
- \*E\* earlier document but published on or after the international filing date
- \*L\* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- \*O\* document referring to an oral disclosure, use, exhibition or other means
- \*P\* document published prior to the international filing date but later than the priority date claimed

- \*T\* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- \*X\* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- \*Y\* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- \*&\* document member of the same patent family

11

Date of the actual completion of the international search

19 September 1997

Date of mailing of the international search report

14.10.97

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentstaan 2  
 NL - 2280 HV Rijswijk  
 Tel. (+ 31-70) 340-2040, Telex 31 651 epo nl,  
 Fax (+ 31-70) 340-3016

Authorized officer

Dupuis, H

# INTERNATIONAL SEARCH REPORT

International Application No  
PCT/CA 97/00269

| C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT |   |                       |
|--|---|-----------------------|
| Category   | Citation of document, with indication, where appropriate, of the relevant passages  | Relevant to claim No. |
| A  | <p>INTERNET SECURITY HANDBOOK,<br/>1995, MAIDENHEAD, ENGLAND,<br/>pages 27-37, XP002040993<br/>STALLINGS W:<br/>see page 31; figure 3.2<br/>-----</p> | 11,24,31              |

# INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No  
PCT/CA 97/00269

| Patent document cited in search report | Publication date | Patent family member(s)  | Publication date                             |
|--|------------------|--|--|
| EP 0465201 A                           | 08-01-92         | US 5309437 A<br>CA 2044363 A<br>DE 69122439 D<br>DE 69122439 T | 03-05-94<br>30-12-91<br>07-11-96<br>15-05-97 |

**THIS PAGE BLANK (USPTO)**